Information-Theoretic Description of No-go Theorem of a Bit Commitment

Yoshihiro Nambu* and Yoshie Chiba-Kohno†
Fundamental Research Laboratories, System Devices and Fundamental Research, NEC Corporation, 34 Miyukigaoka, Tsukuba, Ibaraki 305-8501, Japan
(February 1, 2008)

We give a comprehensive and constructive proof of the no-go theorem of a bit commitment given by Mayers, Lo, and Chau from the viewpoint of quantum information theory. It is shown that there is a trade-off relation between information acquired by Bob during the commitment phase and the ability to change a commit bit by Alice during the opening phase. It is clarified that a protocol that is unbiased to both Alice and Bob cannot be, at the same time, secure against both parties. Fundamental physical constraints that govern this no-go theorem are also discussed.

I. INTRODUCTION

In brief, a bit commitment (BC) is the following task that is executed in two steps ((a) and (b) below) by two mistrustful parties, a sender, Alice, and a receiver, Bob.
(a) Commit phase (C-phase): Alice chooses a bit ($b = 0$ or 1) and commits it to Bob. That is, she gives Bob a piece of evidence that she has a bit b in mind and that she cannot change it (in this case, the commitment is said to be binding). Bob cannot learn the value of the committed bit from that evidence until Alice reveals further information (in this case, the commitment is said to be concealing).
(b) Opening phase (O-phase): At a later time, Alice opens the commitment. That is, she tells Bob the value of b and convinces him that it is indeed the genuine bit that she chose during the C-phase. If Alice changes the value, it can be discovered by Bob.

A BC is an important cryptographic primitive with many applications in more sophisticated tasks and is of great theoretical and practical interest. Current classical BC protocols are proven secure by invoking some unproven computational assumption; that is, complexity of some kind of mathematical problems such as the hardness of factoring large integers. After the invention of the quantum computing algorithm that makes the computational assumption totally invalid, it has been brought to many researchers' attention whether there exists a BC protocol that is guaranteed secure solely by physical principles. In recent years, Mayers, Lo, and Chau have proven that an unconditionally secure BC is impossible (no-go theorem for a BC) under the standard nonrelativistic assumption. [1,2] However, although their discussions are quite correct, their proofs are a bit formal and nonconstructive. It is not yet clear what prevents us from implementing the unconditionally secure BC protocol. In this paper, we give a constructive proof of the no-go theorem for a BC that would make things more transparent and convincing from the viewpoint of quantum information theory. We clarify why quantum mechanics does not help a quantum BC protocol to achieve more than a classical one does.

II. MODEL AND FORMULATION OF THE BIT COMMITMENT PROTOCOL

First, let us consider an honest protocol. The most important point concerning the BC protocol is that Alice needs to unveil a value of b in the O-phase consistently with information transmitted in the C-phase. From the information-theoretic point of view, this implies that one bit of classical information should be transmitted from Alice to Bob at the end of the protocol. Therefore, when we set I_c and I_o as the amounts of information in a bit transmitted in the C-phase and O-phase, the following identity holds:

$$I_c + I_o = 1. \tag{1}$$

Namely, the BC protocol is essentially a split transmission of one-bit information in two temporally separated steps: one in the C-phase and the other in the O-phase. Only a fraction of the bit information needs to be transmitted in each step. Noting this fact, we can formulate the quantum BC protocols reported so far [3–6] as follows.

In order to demand unconditional security, Alice reveals to Bob quantum information as a piece of evidence of her commitment by transmitting a system, such as a photon or an electron, in the C-phase. In the O-phase, she reveals to Bob classical information which consists of the value of b and the measurement basis on the system. Finally, Alice and Bob test the consistency between the reported value of b and the measurement results of the system.

According to the quantum description of the protocol involving classical communication suggested by Tal Mor, let subsystem B (Bob's system) be the system with

arbitrary dimensional state space H_B that carries quantum information in the C-phase and subsystem A (Alice's system) be the system with arbitrary dimensional state space H_A that carries classical information in the O-phase. [7] Let χ_b^{AB} be the genuine states of the joint system AB to be prepared by Alice according to her choice of b. Then, Eq. (1) is equivalent to the condition that χ_0^{AB} and χ_1^{AB} are orthogonal in the joint Hilbert space, $H_{AB} = H_A \otimes H_B$; i.e.,

$$\chi_0^{AB}\chi_1^{AB} = \chi_1^{AB}\chi_0^{AB} = 0. \tag{2}$$

Here, to avoid confusion throughout this paper, we use superscripts to denote the appropriate state space for a state or an operator. According to the protocol, by transmitting a subsystem B to Bob, Alice reveals, in general, nonorthogonal marginal states

$$\rho_b^B = Tr_A \chi_b^{AB} \tag{3}$$

($b = 0$ or 1) in the C-phase. It is proven in Appendix A that from condition (2), we can always find two mutually orthogonal purifications $\left|\psi_b^{AB}\right\rangle$ of ρ_b^B in the orthogonal subspace in which the support of the state χ_b^{AB} lies. Any set of two orthonormal states in H_{AB} should be represented by two orthonormal states in the two-dimensional subspace M spanned by $\left\{\left|0^{AB}\right\rangle, \left|1^{AB}\right\rangle\right\}$ in H_{AB}. Furthermore, any such subspace M can be defined by a set of two orthonormal states in H_{AB}:

$$\begin{aligned} \left|0^{AB}\right\rangle &= \sum \alpha \left|a'^A\right\rangle \left|a^B\right\rangle, \\ \left|1^{AB}\right\rangle &= \sum \beta \left|b'^A\right\rangle \left|b^B\right\rangle, \end{aligned} \tag{4}$$

with an appropriate choice of two sets of orthonormal states $\left\{\left|a'^A\right\rangle \left|a^B\right\rangle\right\}$ and $\left\{\left|b'^A\right\rangle \left|b^B\right\rangle\right\}$ and coefficients α and β, where $\left\{\left\{\left|a'^A\right\rangle\right\}, \left\{\left|b'^A\right\rangle\right\}\right\}$ $\left(\left\{\left\{\left|a^B\right\rangle\right\}, \left\{\left|b^B\right\rangle\right\}\right\}\right)$

makes up a Schmidt basis for H_A (H_B). Therefore, given a set of the mutually orthogonal purifications $\left\{\left|\psi_0^{AB}\right\rangle, \left|\psi_1^{AB}\right\rangle\right\}$ in H_{AB}, we can always find the following form of Schmidt decomposition [8–10],

$$\begin{cases} \left|\psi_0^{AB}\right\rangle = \cos\theta \left|0^{AB}\right\rangle + \sin\theta \left|1^{AB}\right\rangle, \\ \left|\psi_1^{AB}\right\rangle = -\sin\theta \left|0^{AB}\right\rangle + \cos\theta \left|1^{AB}\right\rangle, \end{cases} \tag{5}$$

by choosing appropriate Schmidt coefficients and absorbing any phase factors in the definition of the bases. As a result of Eqs. (4) and (5), the marginal states ρ_0^B and ρ_1^B are commutable and diagonalized simultaneously by Schmidt basis as

$$\begin{aligned} \rho_0^B &= Tr_A \left|\psi_0^{AB}\right\rangle \left\langle\psi_0^{AB}\right| = \cos^2\theta \hat{\rho}_0^B + \sin^2\theta \hat{\rho}_1^B, \\ \rho_1^B &= Tr_A \left|\psi_1^{AB}\right\rangle \left\langle\psi_1^{AB}\right| = \sin^2\theta \hat{\rho}_0^B + \cos^2\theta \hat{\rho}_1^B, \end{aligned} \tag{6}$$

where Tr_A denotes a partial trace over subsystem A, and two states

$$\begin{aligned} \hat{\rho}_0^B &= Tr_A \left|0^{AB}\right\rangle \left\langle 0^{AB}\right| = \sum \alpha^2 \left|a^B\right\rangle \left\langle a^B\right|, \\ \hat{\rho}_1^B &= Tr_A \left|1^{AB}\right\rangle \left\langle 1^{AB}\right| = \sum \beta^2 \left|b^B\right\rangle \left\langle b^B\right|, \end{aligned} \tag{7}$$

are orthogonal on H_B; i.e., $\hat{\rho}_0^B \hat{\rho}_1^B = \hat{\rho}_1^B \hat{\rho}_0^B = 0$. The forms of $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$ can be freely chosen in the protocol and various complex forms have been proposed to prevent cheating of both parties, but the concrete forms are irrelevant to the subject in the following discussion.

III. CHEATING STRATEGIES

According to the model given in Sec II, we will evaluate the performance of Alice's and Bob's cheating.

A. Bob's cheating

The purpose of Bob's cheating is to obtain as much information as possible about b during the C-phase from the marginal states ρ_b^B. In the following, the amount of available information about b for Bob during the C-phase is evaluated as a measure of his cheating performance.

From the protocol agreed by Alice and Bob, the states χ_b^{AB} to be prepared by Alice are known to them. Therefore, Bob can calculate the Schmidt bases, $\left\{\left|a^B\right\rangle\right\}$ and $\left\{\left|b^B\right\rangle\right\}$, that diagonalize the marginal states ρ_0^B and ρ_1^B beforehand. Bob can perform an optimal measurement for distinguishing ρ_0^B and ρ_1^B by making use of the orthogonality between $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$. To describe a measure of the available information about b for Bob from ρ_b^B, consider the fidelity between ρ_0^B and ρ_1^B. [11,12] It is given by

$$F(\rho_0^B, \rho_1^B) = Tr_B \sqrt{\left(\rho_1^B\right)^{1/2} \rho_0^B \left(\rho_1^B\right)^{1/2}}. \tag{8}$$

Noting that $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$ are orthogonal, we can calculate $\left(\rho_1^B\right)^{1/2}$ from Eq. (6) as

$$\left(\rho_1^B\right)^{1/2} = |\sin\theta| \left(\hat{\rho}_0^B\right)^{1/2} + |\cos\theta| \left(\hat{\rho}_1^B\right)^{1/2} \tag{9}$$

in the representation in which $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$ are diagonal. Therefore, Eq. (6) gives

$$F(\rho_0^B, \rho_1^B) = \frac{1}{2} |\sin 2\theta| \, Tr_B \left(\hat{\rho}_0^B + \hat{\rho}_1^B\right) = |\sin 2\theta|. \tag{10}$$

The smaller the fidelity is, the more Bob can distinguish between ρ_0^B and ρ_1^B correctly; therefore, he can gain more information about b. To confirm this, we consider the quantum error probability which gives the lower limit of error rate for distinguishing ρ_0^B and ρ_1^B. [12–14] It is given as

$$P_{err}^{Bob}(\rho_0^B, \rho_1^B) = \frac{1}{2} - \frac{1}{4} Tr_B \left|\rho_0^B - \rho_1^B\right|. \tag{11}$$

Noting again that $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$ are orthogonal, it follows from Eq. (6) that

$$\rho_0^B - \rho_1^B = \cos 2\theta \left(\hat{\rho}_0^B - \hat{\rho}_1^B\right) \tag{12}$$

in the representation in which $\hat{\rho}_0^B$ and $\hat{\rho}_1^B$ are diagonal. Thus, it follows that

$$P_{err}^{Bob}(\rho_0^B, \rho_1^B) = \frac{1 - |\cos 2\theta|}{2} = \frac{1 - \sqrt{1 - \left(F(\rho_0^B, \rho_1^B)\right)^2}}{2}. \tag{13}$$

Let us now introduce distinguishability between ρ_0^B and ρ_1^B as

$$D(\rho_0^B, \rho_1^B) = P_{cor}^{Bob} - P_{err}^{Bob} = \frac{1}{2} Tr_B \left|\rho_0^B - \rho_1^B\right|. \tag{14}$$

Then, the larger the distinguishability is, the more Bob can distinguish between ρ_0^B and ρ_1^B correctly. Thus, the distinguishability gives a measure of the available information about b for Bob from ρ_b^B. It is easily seen that $F(\rho_0^B, \rho_1^B)$ and $D(\rho_0^B, \rho_1^B)$ satisfy

$$\left(F(\rho_0^B, \rho_1^B)\right)^2 + \left(D(\rho_0^B, \rho_1^B)\right)^2 = 1. \tag{15}$$

Therefore, there is a trade-off relationship between $F(\rho_0^B, \rho_1^B)$ and $D(\rho_0^B, \rho_1^B)$; that is, the smaller $F(\rho_0^B, \rho_1^B)$ is, the larger $D(\rho_0^B, \rho_1^B)$ is and the more correctly Bob can distinguish ρ_0^B and ρ_1^B, and vice versa.

Let us turn to the information-theoretic measure of available information for Bob. Mutual information between the value of genuine b and the value of b that is judged from the measurement of ρ_0^B and ρ_1^B is an appropriate measure from the viewpoint of information theory. When Alice chooses the value of commit bit b between 0 and 1 with equiprobability, this measure depends only on ρ_0^B and ρ_1^B and is given by

$$I^{Bob}(\rho_0^B, \rho_1^B) = 1 - H(P_{err}^{Bob}(\rho_0^B, \rho_1^B)), \tag{16}$$

where $H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is an entropy function (in bit).

B. Alice's cheating

The purpose of Alice's cheating is to unveil her commit bit b at her will in the O-phase while ensuring unveiled b does not conflict with Bob's measurement of his subsystem B revealed by her during the C-phase. From the agreed protocol, Alice can calculate the purification given in Eqs. (5) and (4) beforehand.

In the following, her ability to change the commit bit is evaluated for two known cheating strategies as a measure of her cheating performance.

1. Mayer's strategy

This is a strategy which was first proposed by Mayers. [1] Alice honestly reveals either ρ_0^B or ρ_1^B in the C-phase by transmitting subsystem B of the joint system AB prepared in the arbitrary purification associated to either ρ_0^B or ρ_1^B. In the O-phase, by a local unitary operation on subsystem A in her hand, she can change the joint state into any purification $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$ of her chosen ρ_b^B that satisfies

$$\rho_b^B = Tr_A \left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle \left\langle\bar{\psi}_{\bar{b}}^{AB}\right| \tag{17}$$

and

$$0 \leq \left\langle\psi_b^{AB} | \bar{\psi}_{\bar{b}}^{AB}\right\rangle \leq F(\rho_0^B, \rho_1^B), \tag{18}$$

where $\bar{b} = b \oplus 1$. [8,11] Then, according to her necessity, she changes the joint state into the fake states,

$$\begin{aligned} \left|\bar{\psi}_1^{AB}\right\rangle &= -\cos\theta \left|0^{AB}\right\rangle + \sin\theta \left|1^{AB}\right\rangle, \\ \left|\bar{\psi}_0^{AB}\right\rangle &= \sin\theta \left|0^{AB}\right\rangle + \cos\theta \left|1^{AB}\right\rangle. \end{aligned} \tag{19}$$

Here, the state $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$ saturates the upper bound of $\left\langle\psi_b^{AB} | \bar{\psi}_{\bar{b}}^{AB}\right\rangle$ in Eq. (18) and is most parallel to the state $\left|\psi_b^{AB}\right\rangle$. [11] She tells Bob the basis to be used for his measurement on subsystem B that is found from her projection measurement of subsystem A by an appropriate basis $\left\{\left|e_j^A\right\rangle\right\}$. Bob performs projection measurement on his subsystem B according to her instruction and checks her commitment from the consistency between the value of b that is unveiled by Alice in the O-phase and his measurement results.

The fake state $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$ given in Eq. (19) is optimal in Mayer's strategy. To confirm this, we consider the probability P_{err}^{Alice} that Alice causes and Bob finds an inconsistency between the unveiled value of b and Bob's measured data. It is proven in Appendix B that P_{err}^{Alice} is zero when Alice prepares the genuine state χ_b^{AB} or the purification $\left|\psi_b^{AB}\right\rangle$, and

$$P_{err}^{Alice} \geq 1 - \left|\left\langle\psi_b^{AB} | \bar{\psi}_{\bar{b}}^{AB}\right\rangle\right|^2 \tag{20}$$

when she prepares the fake state $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$, where equality holds if and only if $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$ lies in the subspace M spanned by a set of orthonormal states $\left\{\left|0^{AB}\right\rangle, \left|1^{AB}\right\rangle\right\}$. Applying Eq. (18) to Eq. (20) yields

$$P_{err}^{Alice} \geq 1 - \left(F(\rho_0^B, \rho_1^B)\right)^2 = P_{M\,err}^{Alice}(\rho_0^B, \rho_1^B). \tag{21}$$

The state $\left|\bar{\psi}_{\bar{b}}^{AB}\right\rangle$ in Eq. (19) yields the lower bound $P_{M\,err}^{Alice}(\rho_0^B, \rho_1^B)$ for the probability P_{err}^{Alice} that depends only on ρ_0^B and ρ_1^B. Therefore, the fake states in Eq. (19) give the least possibility of disclosing her cheating to Bob and they are optimal for this strategy. The lower limit $P_{M\,err}^{Alice}(\rho_0^B, \rho_1^B)$ is a convenient measure of Alice's ability to change her commitment in the O-phase.

It should be noted that Mayer's strategy is asymmetric with respect to the value of b that Alice unveils in the O-phase. For example, consider Alice reveals ρ_0^B in the C-phase. Then, if she unveils $b = 0$ honestly in the O-phase, Bob's measured data on his subsystem B is perfectly consistent with her disclosure and P_{err}^{Alice} is zero. Conversely, if she wants to unveil $b = 1$, she can cheat Bob successfully with the probability

$$P_{M\ err}^{Alice}(\rho_0^B, \rho_1^B) = \cos^2 2\theta \tag{22}$$

by preparing the fake state $\left|\bar{\psi}_1^{AB}\right\rangle$. Here, Eqs. (10) and (21) are used to derive Eq. (22). Thus, the lower limit $P_{M\ err}^{Alice}(\rho_0^B, \rho_1^B)$ depends on b that Alice unveils in the O-phase. It should be further noted that $P_{M\ err}^{Alice}(\rho_0^B, \rho_1^B) > 1/2$ if $F(\rho_0^B, \rho_1^B) < 1/\sqrt{2}$. This means that Mayer's strategy can be applicable only when $F(\rho_0^B, \rho_1^B) = |\sin 2\theta| \geq 1/\sqrt{2}$.

Now let us turn to the information-theoretic measure of Alice's cheating performance. Let I_M^{Alice} be mutual information between the value of b that Alice unveils and the value of b that Bob judged from his measurement on his subsystem B in the O-phase. Taking into account the asymmetry noted in the previous paragraph, we get the upper bound of I_M^{Alice} as a function only of ρ_0^B and ρ_1^B as follows:

$$I_M^{Alice}(\rho_0^B, \rho_1^B) = \frac{1}{2} + \frac{1}{2}\left\{1 - H(P_{M\ err}^{Alice}(\rho_0^B, \rho_1^B))\right\}. \tag{23}$$

Here, $I_M^{Alice}(\rho_0^B, \rho_1^B)$ is considered to be a good information-theoretic measure of Alice's ability to change her commit bit for this strategy.

2. Hardy-Kent's strategy

This is a strategy which was first given by Koashi and Imoto in the context of quantum key distribution [15], but later applied to the BC protocol by Hardy and Kent. [6] According to this strategy, Alice reveals $\bar{\rho}^B = \left(\rho_0^B + \rho_1^B\right)/2$ in the C-phase by transmitting the subsystem B of the joint system AB prepared in the arbitrary purification of $\bar{\rho}^B$. When she unveils her commitment in the O-phase, she can change the joint state into any purification $\left|\bar{\psi}_b^{AB}\right\rangle$ of $\bar{\rho}^B$ satisfying

$$\bar{\rho}^B = Tr_A \left|\bar{\psi}_b^{AB}\right\rangle \left\langle\bar{\psi}_b^{AB}\right| \tag{24}$$

and

$$0 \leq \left\langle\psi_b^{AB}|\bar{\psi}_b^{AB}\right\rangle \leq F(\rho_b^B, \bar{\rho}^B) \tag{25}$$

by performing a local unitary operation on her subsystem A. Then, according to her choice of b, she changes the joint state into the fake state, for example, so that when $0 \leq \theta \leq \pi/2$,

$$\begin{aligned}\left|\bar{\psi}_0^{AB}\right\rangle &= \left(\left|0^{AB}\right\rangle + \left|1^{AB}\right\rangle\right)/\sqrt{2},\\ \left|\bar{\psi}_1^{AB}\right\rangle &= -\left(\left|0^{AB}\right\rangle - \left|1^{AB}\right\rangle\right)/\sqrt{2}.\end{aligned} \tag{26}$$

Here, $\left|\bar{\psi}_b^{AB}\right\rangle$ saturates the upper bound of $\left\langle\psi_b^{AB}|\bar{\psi}_b^{AB}\right\rangle$ in Eq. (25) and is the most parallel to the state $\left|\psi_b^{AB}\right\rangle$. [11] She tells Bob the basis to be used for his measurement on subsystem B that is found from her projection measurement on her subsystem A by an appropriate basis $\left\{\left|e_j^A\right\rangle\right\}$. Bob performs projection measurement on his system according to her instruction and checks her commitment from the consistency between the value of b that is unveiled by Alice in the O-phase and his measurement results.

It can also be proven from Appendix B that the lower bound $P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)$ of the probability P_{err}^{Alice} in this strategy depends only on ρ_0^B and ρ_1^B, and it is given by

$$P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B) = 1 - \left(F(\rho_b^B, \bar{\rho}^B)\right)^2 = \frac{1 - F(\rho_0^B, \rho_1^B)}{2}. \tag{27}$$

The states $\left|\bar{\psi}_b^{AB}\right\rangle$ in Eq. (26) yield the lower bound $P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)$. Therefore, they are optimal for this strategy. The lower limit $P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)$ gives a convenient measure of Alice's ability to change her commitment in the O-phase.

In contrast to Mayer's strategy, Hardy-Kent's strategy is symmetric with respect to the value of b that Alice unveils in the O-phase. The lower limit $P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)$ is independent of her disclosure of b. The upper bound of the mutual information I_{HK}^{Alice} for Hardy-Kent's strategy is written in terms of $P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)$ as

$$I_{HK}^{Alice}(\rho_0^B, \rho_1^B) = 1 - H(P_{HK\ err}^{Alice}(\rho_0^B, \rho_1^B)), \tag{28}$$

which is considered to be a good information-theoretic measure of Alice's ability to change commit bit b in this strategy.

To compare the cheating performances of Alice and Bob for both Mayer's and Hardy-Kent's strategies, we plot the three information theoretic measures $I^{Bob}(\rho_0^B, \rho_1^B)$, $I_M^{Alice}(\rho_0^B, \rho_1^B)$, and $I_{HK}^{Alice}(\rho_0^B, \rho_1^B)$ in Fig. 1 as a function of the fidelity $F(\rho_0^B, \rho_1^B)$ chosen as a common parameter. This figure clearly shows that there is a trade-off relationship between Bob's available information in the C-phase ($I^{Bob}(\rho_0^B, \rho_1^B)$) and Alice's ability to change commit bit b in the O-phase ($I_i^{Alice}(\rho_0^B, \rho_1^B)$). It is clear that the sum is bounded; i.e.,

$$I^{Bob}(\rho_0^B, \rho_1^B) + I_i^{Alice}(\rho_0^B, \rho_1^B) \leq 1 \tag{29}$$

(for $i = M, HK$). This equation is a direct consequence of Eq. (15), showing a trade-off relationship between the distinguishability $D(\rho_0^B, \rho_1^B)$, a measure of Bob's information gain in the C-phase, and the fidelity $F(\rho_0^B, \rho_1^B)$, a measure of Alice's ability to change commit bit in the

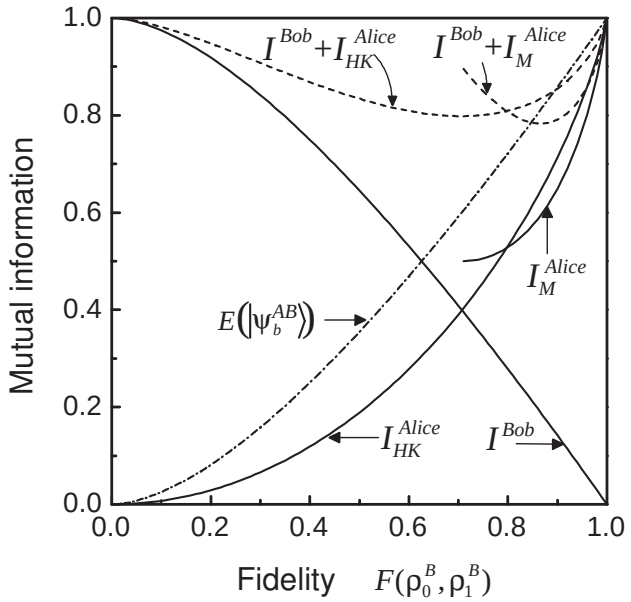

FIG. 1. Three information-theoretic measures $I^{Bob}(\rho_0^B, \rho_1^B)$, $I_M^{Alice}(\rho_0^B, \rho_1^B)$, and $I_{HK}^{Alice}(\rho_0^B, \rho_1^B)$ are plotted against fidelity $F(\rho_0^B, \rho_1^B)$. Entropy of entanglement $E\left(|\psi_b^{AB}\rangle\right)$ is also plotted for reader's information.

O-phase. Therefore, there is a trade-off in the performance of Alice's and Bob's cheating. Figure 1 also shows that Hardy-Kent's strategy is superior to Mayer's with respect to ability to change commit bit b when the value of $F(\rho_0^B, \rho_1^B)$ is large.

IV. DISCUSSION

A secure BC protocol must not allow cheating by either parties, Alice or Bob. To satisfy this condition, both $I^{Bob}(\rho_0^B, \rho_1^B)$ and $I_i^{Alice}(\rho_0^B, \rho_1^B)$ should vanish simultaneously. However, Fig. 1 indicates that this requirement is never satisfied because of the trade-off relationship between $I^{Bob}(\rho_0^B, \rho_1^B)$ and $I_i^{Alice}(\rho_0^B, \rho_1^B)$. In addition, even if we choose a balanced condition for both parties, $F(\rho_0^B, \rho_1^B) \sim 1/\sqrt{2}$, both $I^{Bob}(\rho_0^B, \rho_1^B)$ and $I_i^{Alice}(\rho_0^B, \rho_1^B)$ are already large enough. Therefore, it is concluded that a law of quantum physics does not help to improve the security of the BC protocol.

As already proven generally by Mayers, Lo, and Chau, this conclusion should be valid not only for the particular cheating strategies described in this paper but also for any strategies that Alice and Bob can choose. To understand this conclusion, consider the entropy of entanglement (or entanglement in brief), which is known to be a unique measure of the amount of entanglement for the pure state. [10,16,17] Entanglement of the purification $|\psi_b^{AB}\rangle$ is defined as the von Neumann entropy of the marginal state ρ_b^B of $|\psi_b^{AB}\rangle$ or equivalently as the Shannon entropy of the squares of the Schmidt coefficients of $|\psi_b^{AB}\rangle$. From Eqs. (5), (4), (13), and (16), it is easily calculated as

$$E\left(|\psi_b^{AB}\rangle\right) = S\left(\rho_b^B\right) = 1 - I^{Bob}(\rho_0^B, \rho_1^B). \tag{30}$$

Here, it should be noted that $I^{Bob}(\rho_0^B, \rho_1^B)$ is equivalent to maximum information I_c available from ρ_b^B that is transmitted from Alice to Bob in the C-phase; that is,

$$I_c = I^{Bob}(\rho_0^B, \rho_1^B) = 1 - E\left(|\psi_b^{AB}\rangle\right). \tag{31}$$

Applying Eqs. (1) and (29) to (31), we obtain the inequality,

$$I_i^{Alice}(\rho_0^B, \rho_1^B) \leq E\left(|\psi_b^{AB}\rangle\right) = I_o. \tag{32}$$

This inequality implies two things. First, the performance of Alice's cheating, when it is measured by $I_i^{Alice}(\rho_0^B, \rho_1^B)$, is bounded by the entanglement of the purification $E\left(|\psi_b^{AB}\rangle\right)$, which is determined only by its marginal state ρ_b^B (see Eq. (30)). Second, it is also bounded by the amount of information I_o that is revealed in the O-phase.

These implications are reasonable for the following reason. When Alice wants to cheat Bob, what she can do is restricted to local operation and measurement on the subsystem A in her hand after she has revealed ρ_b^B by transmitting the subsystem B. It is known to be a fundamental law of quantum information processing that entanglement cannot be increased if we are allowed to perform only local operations and subselection on the subsystem of a joint system. In this restricted situation, the best she can do to cheat is use the local unitary operation that conserves the entanglement shared in the joint system and keeps the marginal states ρ_b^B unchanged. Otherwise, the strategy must be by far an optimal one because a fraction of the entanglement must be lost from the joint system and dissipate into the environment during the local operation. Under such circumstances, Alice can change the information content encoded only in the relative phase between coefficients of each term in the purification $|\psi_b^{AB}\rangle$, but she cannot change the information content encoded in their absolute values. It is the entanglement resource that is responsible for Alice's cheating, and there is no cheating strategy that can break the bound given by entanglement $E\left(|\psi_b^{AB}\rangle\right)$ as shown in Eq. (32). In addition, it is also reasonable that only partial information that is to be revealed in the O-phase can be used for Alice's cheating but the partial information already revealed in the C-phase cannot. Conversely, we must be aware that Alice makes use of partial information that is reserved to be revealed in the O-phase as an entanglement resource for cheating.

It is worth noting that the present proof can be regarded as a concrete example of the general proof of the no-go theorem for a zero-knowledge-convincing protocol

recently given by Horodecki et al. [18] Our proof clearly indicates that if Alice wants to convince Bob that she has a definite value of a commit bit (which is, of course, *classical* information) in mind in the C-phase, the information provided by her to him in the C-phase has to carry nontrivial information about the commit bit in her mind. If the information revealed in the C-phase is independent of her commit bit, Alice can always try to cheat by proposing the test which would give some result with certainty and independently of her commit bit in the O-phase. Our proof suggests an information-theoretic ground for the no-go theorem of the zero-knowledge-convincing protocol. Namely, any protocol with a test message that convinces Bob that Alice knows some state ϕ (which is, in general, *quantum* information), the test message has to carry non-zero information about state ϕ to prevent Alice's cheating.

The present proof implies that the conjecture of Mayers about two-party secure computation, which states that the symmetric protocol might be possible whereas the asymmetric tasks, such as unidirectional secure computations, would be impossible, is correct. [1] In the unidirectional two-party computation, which allows only one of the two parties to learn the result, both members of the party can be a cheater and security requirements for both members are incompatible. Such unidirectional protocols under the standard nonrelativistic assumption are necessarily insecure. We believe that unidirectional quantum communication does not achieve more than classical communication alone in the two-party model. However, it has not yet been proven that no non-trivial cryptographic tasks in the two-party model using bidirectional quantum communication are unconditionally secure. Indeed, there are some proposals on the quantum protocols for non-trivial weaker tasks in two-party bidirectional quantum communication such as quantum coin-tossing [19] and quantum gambling. [20] It will still be important to solve the general problem concerning what is possible and what is impossible in two-party secure computation when unproven computational assumptions are abandoned.

V. CONCLUSIONS

In conclusion, we have given constructive proof why an unconditionally secure quantum BC is impossible in the light of quantum information theory. The BC protocol is in essence the protocol in which one-bit information is split and revealed in two temporally separated steps: the C-phase and the O-phase. It ensures only a fraction of the bit information is revealed at a time. In the quantum BC protocol, increasing the information revealed in the C-phase is to Bob's advantage; conversely, increasing the information revealed in the O-phase makes things to Alice's advantage. This situation is similar to the classical protocol. Furthermore, the protocol that is unbiased to both Alice and Bob is not secure for both. Therefore, it is impossible to design a BC protocol whose security is established solely on the law of quantum physics.

In addition, it has been clarified that, Alice can make use of the entanglement resource, which is equal to the amount of information reserved to be revealed in the O-phase, to cheat. To prevent Alice's cheating, the information revealed in the C-phase must depend on her commit bit, and it must inevitably carry non-zero information about her commitment. It can be concluded that quantum mechanics itself makes designing an unconditionally secure BC protocol impossible.

APPENDIX A: A PROOF OF EXISTENCE OF MUTUALLY ORTHOGONAL PURIFICATIONS OF ρ_b^B

Suppose that the states χ_b^{AB} $(b = 0, 1)$ of joint system AB that is to be prepared by Alice are mutually orthogonal on the joint space $H_{AB} = H_A \otimes H_B$; i.e.,

$$\chi_0^{AB}\chi_1^{AB} = \chi_1^{AB}\chi_0^{AB} = 0. \tag{A1}$$

Because χ_0^{AB} and χ_1^{AB} commute, they can be diagonalized simultaneously in terms of orthonormal bases $\{|e^{AB}\rangle\}$ and $\{|f^{AB}\rangle\}$ in H_{AB} as follows:

$$\begin{aligned}\chi_0^{AB} &= \sum \lambda_e \left|e^{AB}\right\rangle \left\langle e^{AB}\right|, \\ \chi_1^{AB} &= \sum \lambda_f \left|f^{AB}\right\rangle \left\langle f^{AB}\right|, \end{aligned} \tag{A2}$$

where $\{|e^{AB}\rangle\}$ and $\{|f^{AB}\rangle\}$ are mutually orthogonal; i.e., $\langle e^{AB}|f^{AB}\rangle = \langle f^{AB}|e^{AB}\rangle = 0$, and $\{\lambda_e\}$ and $\{\lambda_f\}$ are sets of real eigenvalues of χ_b^{AB} satisfying $0 \le \lambda_e, \lambda_f \le 1$ and $\sum \lambda_e = \sum \lambda_f = 1$. Thus, χ_0^{AB} and χ_1^{AB} have orthogonal supports in H_{AB}. Marginal states revealed by Alice to Bob in the C-phase are commutable and, in general, nonorthogonal states. Using this representation, we can write them as

$$\begin{aligned}\rho_0^B = Tr_A\chi_0^{AB} &= \sum \lambda_e Tr_A \left|e^{AB}\right\rangle \left\langle e^{AB}\right|, \\ \rho_1^B = Tr_A\chi_1^{AB} &= \sum \lambda_f Tr_A \left|f^{AB}\right\rangle \left\langle f^{AB}\right|. \end{aligned} \tag{A3}$$

Now, we consider mutually orthonormal states $|\psi_0^{AB}\rangle$ and $|\psi_1^{AB}\rangle$ $(\langle\psi_0^{AB}|\psi_1^{AB}\rangle = 0)$ that lie in the subspace to which χ_0^{AB} and χ_1^{AB} belong respectively; i.e.,

$$\begin{aligned}\left|\psi_0^{AB}\right\rangle &= \sum c_e \left|e^{AB}\right\rangle, \\ \left|\psi_1^{AB}\right\rangle &= \sum c_f \left|f^{AB}\right\rangle. \end{aligned} \tag{A4}$$

Then, the marginal states for them are

$$\begin{aligned} Tr_A \left|\psi_0^{AB}\right\rangle \left\langle\psi_0^{AB}\right| &= \sum \left|c_e\right|^2 Tr_A \left|e^{AB}\right\rangle \left\langle e^{AB}\right| \\ &\quad + \sum c_e c_{e'}^* Tr_A \left|e^{AB}\right\rangle \left\langle e'^{AB}\right|, \\ Tr_A \left|\psi_1^{AB}\right\rangle \left\langle\psi_1^{AB}\right| &= \sum \left|c_f\right|^2 Tr_A \left|f^{AB}\right\rangle \left\langle f^{AB}\right| \\ &\quad + \sum c_f c_{f'}^* Tr_A \left|f^{AB}\right\rangle \left\langle f'^{AB}\right|. \end{aligned} \tag{A5}$$

Because the states of subsystem A represent the classical information transferred from Alice to Bob in the O-phase, different states $\left|e^{AB}\right\rangle \neq \left|e'^{AB}\right\rangle$ and $\left|f^{AB}\right\rangle \neq \left|f'^{AB}\right\rangle$ are orthogonal on the subspace H_A. Therefore,

$$Tr_A \left|e^{AB}\right\rangle \left\langle e'^{AB}\right| = Tr_A \left|f^{AB}\right\rangle \left\langle f'^{AB}\right| = 0. \quad \text{(A6)}$$

By noting that the second terms in Eq. (A5) vanishes, it is concluded that by choosing c_e and c_f so that

$$\begin{aligned} \lambda_e &= |c_e|^2, \\ \lambda_f &= |c_f|^2, \end{aligned} \quad \text{(A7)}$$

it is always possible to obtain mutually orthogonal purification $\left|\psi_b^{AB}\right\rangle$ of ρ_b^{AB} in the subspace in which the support of the state χ_b^{AB} lies.

APPENDIX B: PROBABILITY THAT BOB DETECTS ALICE'S CHEATING

Suppose that the state of subsystem A is measured to be $\left|e_j^A\right\rangle$ when A of the joint system AB prepared in the state $\left|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}\right|$ is subjected to projection measurement by the orthonormal basis $\left\{\left|e_j^A\right\rangle\right\}$ for H_A. According to general results of quantum measurement theory, the state of the subsystem B is projected onto the pure state

$$\rho_b^B \left(\left|e_j^A\right\rangle\right) = \frac{\left\langle e_j^A|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}|e_j^A\right\rangle}{Tr_B \left\langle e_j^A|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}|e_j^A\right\rangle}. \quad \text{(B1)}$$

From Eqs. (5) and (4), it is easily seen that

$$\begin{aligned} \left\langle\psi_0^{AB}|e_j^A\right\rangle \left\langle e_j^A|\psi_1^{AB}\right\rangle = \frac{\sin 2\theta}{2} &\left(\left\langle 1^{AB}|e_j^A\right\rangle \left\langle e_j^A|1^{AB}\right\rangle\right. \\ &\left. - \left\langle 0^{AB}|e_j^A\right\rangle \left\langle e_j^A|0^{AB}\right\rangle\right). \end{aligned} \quad \text{(B2)}$$

Therefore, we find that, if and only if the basis $\left\{\left|e_j^A\right\rangle\right\}$ is chosen so that the overlap between $\left|e_j^A\right\rangle$ and $\left|0^{AB}\right\rangle$ and that between $\left|e_j^A\right\rangle$ and $\left|1^{AB}\right\rangle$ are the same, i.e.,

$$\left\langle 0^{AB}|e_j^A\right\rangle \left\langle e_j^A|0^{AB}\right\rangle = \left\langle 1^{AB}|e_j^A\right\rangle \left\langle e_j^A|1^{AB}\right\rangle, \quad \text{(B3)}$$

the states $\rho_0^B \left(\left|e_j^A\right\rangle\right)$ and $\rho_1^B \left(\left|e_j^A\right\rangle\right)$ become mutually orthogonal. In the quantum BC protocol, Alice and Bob agree to use the measurement basis $\left\{\rho_0^B \left(\left|e_j^A\right\rangle\right), \rho_1^B \left(\left|e_j^A\right\rangle\right)\right\}$ on subsystem B that has a one-to-one correspondence to a state $\left|e_j^A\right\rangle$ on A through the joint state $\left|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}\right|$. She reveals to Bob the measurement basis $\left\{\rho_0^B \left(\left|e_j^A\right\rangle\right), \rho_1^B \left(\left|e_j^A\right\rangle\right)\right\}$ associated with her state $\left|e_j^A\right\rangle$ in the O-phase, and he measures his subsystem B by this basis.

Now, we consider the probability P_{err}^{Alice} that Alice causes an inconsistency between the value of b that is unveiled by her in the O-phase and Bob's measured data when Alice prepares an honest state χ_b^{AB}. Alice projects her subsystem A of the joint system AB prepared in χ_b^{AB} onto a state $\left|e_j^A\right\rangle$ among the complete orthonormal basis $\left\{\left|e_j^A\right\rangle\right\}$ for space H_A. She can perform such a projection on her subsystem at her own free will. Correspondingly, the state of Bob's system is projected to be

$$\tilde{\rho}_b^B \left(\left|e_j^A\right\rangle\right) = \frac{\left\langle e_j^A\right| \chi_b^{AB} \left|e_j^A\right\rangle}{Tr_B \left\langle e_j^A\right| \chi_b^{AB} \left|e_j^A\right\rangle}. \quad \text{(B4)}$$

Here, from Appendix A, the states $\left|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}\right|$ and χ_b^{AB} satisfy

$$\left\langle e_j^A|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}|e_j^A\right\rangle = \left\langle e_j^A\right| \chi_b^{AB} \left|e_j^A\right\rangle. \quad \text{(B5)}$$

Then, we obtain the identity $\rho_b \left(\left|e_j^A\right\rangle\right) = \tilde{\rho}_b \left(\left|e_j^A\right\rangle\right)$. This identity implies that if Bob follows Alice's instruction and measures his system by the measurement basis given by her, the value of b unveiled by Alice in the O-phase is perfectly correlated with Bob's measurement result, no matter what Alice prepares $\left|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}\right|$ or χ_b^{AB}. Therefore, if Bob is honest enough to follow Alice's instruction, the probability P_{err}^{Alice} that Bob finds an inconsistency in his data vanishes if Alice prepares $\left|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}\right|$ or χ_b^{AB}. Consequently, Alice can transmit one bit of classical information to Bob with certainty.

Next, we consider the probability P_{err}^{Alice} when Alice prepares a fake state $\left|\bar{\psi}^{AB}\right\rangle$ that lies in joint space H_{AB}. When the joint system AB prepared in the state $\left|\bar{\psi}^{AB}\right\rangle \left\langle\bar{\psi}^{AB}\right|$ is subjected to the projection measurement by using the orthonormal basis $\left\{\left|e_j^A\right\rangle\right\}$ for H_A and the result is $\left|e_j^A\right\rangle$, the state of the subsystem B is projected onto the pure state

$$\bar{\rho}^B \left(\left|e_j^A\right\rangle\right) = \frac{\left\langle e_j^A|\bar{\psi}^{AB}\right\rangle \left\langle\bar{\psi}^{AB}|e_j^A\right\rangle}{Tr_B \left\langle e_j^A|\bar{\psi}^{AB}\right\rangle \left\langle\bar{\psi}^{AB}|e_j^A\right\rangle}. \quad \text{(B6)}$$

Let the fidelity between $\bar{\rho}^B \left(\left|e_j^A\right\rangle\right)$ and $\rho_b^B \left(\left|e_j^A\right\rangle\right)$ be $F\left(\bar{\rho}^B \left(\left|e_j^A\right\rangle\right), \rho_b^B \left(\left|e_j^A\right\rangle\right)\right)$. Then, the probability P_{err}^{Alice} that Bob finds an inconsistency in his data is given by

$$P_{err}^{Alice} = 1 - \left|F\left(\bar{\rho}^B \left(\left|e_j^A\right\rangle\right), \rho_b^B \left(\left|e_j^A\right\rangle\right)\right)\right|^2. \quad \text{(B7)}$$

Under the condition of Eq. (B3), it follows that

$$\begin{aligned} \left\langle\psi^{AB}|e_j^A\right\rangle \left\langle e_j^A|\psi_b^{AB}\right\rangle = \frac{1}{2} &Tr_{AB}\left|e_j^A\right\rangle \left\langle e_j^A\right| P_M \\ &\cdot \left\langle\psi^{AB}|\psi_b^{AB}\right\rangle, \end{aligned} \quad \text{(B8)}$$

$$\begin{aligned} Tr_B \left\langle e_j^A|\psi^{AB}\right\rangle \left\langle\psi^{AB}|e_j^A\right\rangle &= Tr_B \left\langle e_j^A|\psi_b^{AB}\right\rangle \left\langle\psi_b^{AB}|e_j^A\right\rangle \\ &\geq \frac{1}{2} Tr_{AB} \left|e_j^A\right\rangle \left\langle e_j^A\right| P_M, \end{aligned} \quad \text{(B9)}$$

where $P_M = \left|0^{AB}\right\rangle \left\langle 0^{AB}\right| + \left|1^{AB}\right\rangle \left\langle 1^{AB}\right|$ is the projector onto two-dimensional subspace M in H_{AB} that is spanned by a set of orthonormal states $\left\{\left|0^{AB}\right\rangle, \left|1^{AB}\right\rangle\right\}$,

and $Tr_{AB}\left|e_j^A\right\rangle\left\langle e_j^A\right| P_M = \left\langle 0^{AB}|e_j^A\right\rangle\left\langle e_j^A|0^{AB}\right\rangle + \left\langle 1^{AB}|e_j^A\right\rangle\left\langle e_j^A|1^{AB}\right\rangle$ is the overlap between the state $\left|e_j^A\right\rangle$ in H_A and subspace M. The equal sign in inequality (B9) holds if and only if state $\left|\bar{\psi}^{AB}\right\rangle$ lies within subspace M.

From Eqs. (B1),(B6),(B8), and (B9), we obtain

$$\left|F\left(\bar{\rho}^B\left(\left|e_j^A\right\rangle\right), \rho_b^B\left(\left|e_j^A\right\rangle\right)\right)\right|^2 \leq \left|\left\langle\psi^{AB}|\psi_b^{AB}\right\rangle\right|^2. \quad \text{(B10)}$$

Applying Eq. (B10) to Eq. (B7), we finally obtain

$$P_{err}^{Alice} \geq 1 - \left|\left\langle\psi^{AB}|\psi_b^{AB}\right\rangle\right|^2. \quad \text{(B11)}$$

Here, equality holds if and only if the state $\left|\bar{\psi}^{AB}\right\rangle$ lies within subspace M.

---

* Electronic address: y-nambu@ah.jp.nec.com

† Present address: ATR Adaptive Communications Research Labs., 2-2-2 Hikaridai, Seika-cho, Soraku-gun, Kyoto 619-0288, Japan
Electronic address: kohno@acr.atr.co.jp

[1] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[2] H-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India 1984* (IEEE, New York, 1984), p. 175-179.

[4] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, in *Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science* (IEEE Computer Society Press, Los Alamitos, California 1993), p. 362-371.

[5] G. Brassard, C. Crépeau, D. Mayers, L. Salvail, quant-ph/9712023.

[6] L. Hardy and A. Kent, quant-ph/9911043.

[7] Tal Mor, Phys. Rev. Lett. **80**, 3137 (1998).

[8] L. P. Hughston, R. Jozsa, and W. K. Wootters, Phys. Lett. **A 183**, 14-18 (1993).

[9] A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).

[10] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. **A 44**, 535 (1991).

[11] R. Jozsa, J. Mod. Opt. **41**, 2315-2323 (1994).

[12] C. A. Fuchs, quant-ph/9601020.

[13] C. A. Fuchs, quant-ph/9611010.

[14] C. W. Helstrom, *Quantum detection and estimation theory* (Academic, New York, 1976).

[15] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).

[16] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. **A 53**, 2046 (1996).

[17] M. B. Plenio and V. Vedral, Contemp. Phys. **39**, 431 (1998).

[18] P. Horodecki, M. Horodecki, and R. Horodecki, quant-ph/0010048.

[19] D. Mayers, L. Salvail, and Y. Chiba-Kohno, quant-ph/9904078.

[20] L. Goldenberg, L. Vaidman, and S. Wiesner, Phys. Rev. Lett. **82**, 3356 (1999).